

Authenticating objects and object data involves encoding identification data based on interrogation of object identifier(s) together with recorded image to produce combination data

Patent number: DE19960769

Publication date: 2000-06-29

Inventor: CHAINER TIMOTHY JOSEPH [US]; GREENGARD
CLAUDE A [US]; MOSKOWITZ PAUL ANDREW [US]

Applicant: IBM [US]

Classification:

- international: G07C11/00; G01S13/74

- european: G01S17/88; H04N1/00C; H04N1/32C

Application number: DE19991060769 19991216

Priority number(s): US19980213179 19981217

Also published as:

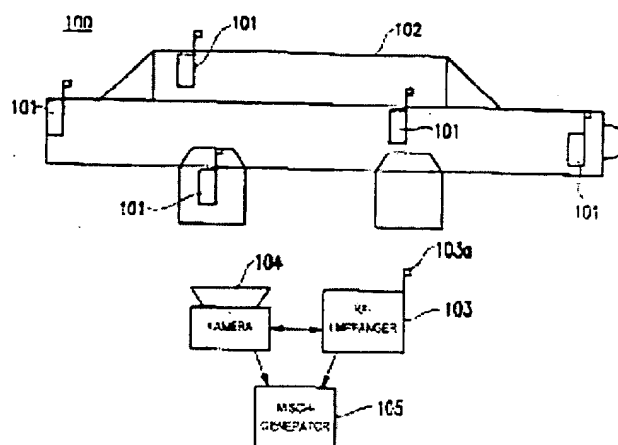


US6397334 (B1)

JP2000261751 (A)

Abstract of DE19960769

The method involves associating at least one identifier with the object (102), interrogating (101) the identifier(s) to produce identification data, recording (104) an image of the object including the identifier(s) and encoding (107) the identification data based on the interrogation of the identifier(s) together with the recorded image to produce combination data.. An Independent claim is also included for a system for authenticating objects and object data.



Data supplied from the esp@cenet database - Worldwide



①9 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑫ **Offenlegungsschrift**
⑩ **DE 199 60 769 A 1**

⑤1 Int. Cl.7:
G 07 C 11/00
G 01 S 13/74

②1 Aktenzeichen: 199 60 769.9
②2 Anmeldetag: 16. 12. 1999
④3 Offenlegungstag: 29. 6. 2000

DE 199 60 769 A 1

③0 Unionspriorität:
213179 17. 12. 1998 US
⑦1 Anmelder:
IBM Corp., Armonk, N.Y., US
⑦4 Vertreter:
Teufel, F., Dipl.-Phys., Pat.-Anw., 70569 Stuttgart

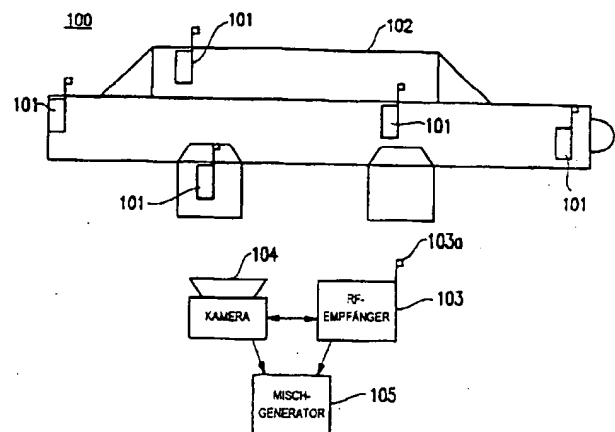
⑦2 Erfinder:
Chainer, Timothy Joseph, Mahopac, N.Y., US;
Greengard, Claude A., Chappaqua, N.Y., US;
Moskowitz, Paul Andrew, Yorktown Heights, N.Y., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Verfahren und System zur Authentifizierung von Objekten und Objektdaten

⑤7 Ein System und Verfahren zur Authentifizierung eines Bildes von einem Objekt enthält mindestens eine dem Objekt zugeordnete Kennung, einen Empfänger zum Abfragen der mindestens einen Kennung, um Identifikationsdaten zu erzeugen, ein Kamerasystem zum Aufzeichnen eines Bildes von dem Objekt einschließlich des mindestens einen Kennzeichens, und einen Mischgenerator zum Codieren der Identifikationsdaten vom Empfänger zusammen mit dem vom Kamerasystem aufgenommenen Bild, um Kombidaten zu erzeugen.



DE 199 60 769 A 1

Beschreibung

HINTERGRUND DER ERFINDUNG

Gegenstand der Erfindung

Die vorliegende Erfindung betrifft allgemein ein Verfahren und System zur Authentifizierung von Objekten und Objektdaten.

Stand der Technik

Es wurden bereits zahlreiche Versuche unternommen, belebte und unbelebte Objekte zu fälschen. Ein besonders bedeutendes Problem, mit dem Versicherungsunternehmen konfrontiert sind, ist die Fälschung von Schäden und Reparaturen, vor allem, aber nicht ausschließlich, an Kraftfahrzeugen (z. B. PKWs, LKWs, Motorrädern usw.).

Oft werden Fahrzeuge nach einem Unfall zu einer Werkstatt gebracht, und der Schaden wird fotografiert. Dann wird nach der angeblichen Reparatur noch einmal fotografiert. Das zweite Foto wird dann den Versicherungsunternehmen vorgelegt, um das Geld zu kassieren. Manchmal ist aber das zweite Foto (oder das erste und das zweite Foto) verändert ("frisiert") worden, oder die Fotos zeigen ein anderes Fahrzeug.

Auf diese Weise wird das Versicherungsunternehmen von der skrupellosen Werkstatt und/oder dem Fahrzeugbesitzer betrogen.

Außerdem gibt es bei manchen konventionellen Systemen kein Verfahren, das verhindert (oder zumindest erkennt), daß ein Objekt fotografiert wird, das gar nicht dasjenige ist, für das es gehalten werden sollte (z. B. für Versicherungszwecke).

Es gibt zum Beispiel kein Verfahren, mit dem man erkennen kann, daß ein Foto von einem Fahrzeug in einwandfreiem Zustand (z. B. unbeschädigt) gemacht wird, das ähnlich aussieht wie ein Fahrzeug, das in einen Unfall verwickelt war, und dieses Foto dann an das Versicherungsunternehmen geschickt wird, um das Geld für eine in Wirklichkeit gar nicht ausgeführte Reparatur zu kassieren.

Eine Lösung des geschilderten Problems erfordert, daß das von einer Kamera aufgenommene Foto ein authentisches Foto ist (z. B. ein Foto, das nicht verändert worden ist). In einem konventionellen System gibt es eine Vorrichtung, die die von einer digitalen Kamera aufgenommenen Bilder authentifiziert, indem eine digitale Signatur codiert und dem Bild hinzugefügt wird.

In einem solchen System verwendet die digitale Kamera kryptographische Mittel, um eine Signatur zur Authentifizierung der erzeugten Bilder zu erzeugen. Und zwar wird dem Bild eine codierte Nachricht hinzugefügt, um die Authentifizierung zu ermöglichen. Dem Bild können auch noch weitere Informationen hinzugefügt werden. Das konventionelle System mit einer solchen digitalen Kamera kann aber nicht alle Formen des Betrugs zuverlässig verhindern (oder zumindest erkennen). Das konventionelle System wäre beispielsweise nicht in der Lage, die oben geschilderten betrügerischen Aktivitäten zu verhindern.

Erstens kann das Bild, das der digitalen Kamera präsentiert wird, eine Fotografie sein, und es muß nicht notwendigerweise das tatsächliche Bild vom Zustand des Objekts (z. B. des Fahrzeugs) sein. Ein solches Foto könnte ohne weiteres verändert worden sein.

Zweitens könnten die Zusatzinformationen wie z. B. Temperatur usw., die dem Bild hinzugefügt werden, von einer anderen Quelle stammen, und es könnte über verschiedene Zwischenstationen so arrangiert werden, daß der An-

schein erweckt wird, sie kämen von der digitalen Kamera. Auch wenn also das konventionelle System einige der erwähnten Problemen lösen kann, z. B. Retuschieren und ähnliches, bleiben immer noch ein paar Nachteile. So können solche Systeme beispielsweise nicht zwischen ähnlichen Gegenständen unterscheiden, wie sie in der Massenproduktion entstehen (z. B. bei Unterhaltungselektronik wie Fernsehgeräten, Videorecordern u. a., bei Kraftfahrzeugen wie PKWs, Motorrädern und Booten, bei Kunstwerken, teuren Kleidungsstücken usw.).

Betrügerische Machenschaften werden nicht zuverlässig verhindert, wodurch den Versicherungsunternehmen (und damit letztlich den ehrlichen Versicherungskunden) Kosten in Höhe von mehreren hundert Millionen Dollar pro Jahr entstehen.

ÜBERBLICK ÜBER DIE ERFINDUNG

Angesichts der erwähnten und anderer Probleme der konventionellen Systeme und Verfahren ist es eine Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System bereit zustellen, das die Unterbreitung gefälschter Bilder verhindert, und speziell die falsche Präsentation z. B. von Schäden und nachfolgenden Reparaturen.

Eine andere Aufgabe der vorliegenden Erfindung besteht darin, eine Struktur und ein Verfahren bereitzustellen, in denen eine Kamera und ein Lesegerät (z. B. ein Radiofrequenz-Lesegerät (RF-Lesegerät)) kombiniert sind, die gleichzeitig sowohl ein Bild eines Objekts als auch eine Bitfolge, die mindestens einem Kennzeichen des Objekts zugeordnet ist und der Kennung des Objekts entspricht, aufzeichnet.

Eine weitere Aufgabe ist die Bereitstellung eines Systems und eines Verfahrens zur Authentifizierung von Daten, die angeblich mit einem physischen Objekt verknüpft sind, indem mehr als eine Art von Information über das Objekt verwendet und auf sichere Weise gespeichert wird. Dieses System und Verfahren kann in Kombination mit einer Fotografie zur Authentifizierung des digitalen Bildes verwendet werden.

In einem ersten Aspekt enthält ein System zur Authentifizierung eines Bildes von einem Objekt mindestens eine Kennung des Objekts, einen Empfänger zur Abfrage der mindestens einen Kennung, ein Kamerasystem zum Aufzeichnen eines Bildes von dem Objekt einschließlich der mindestens einen Kennung, und einen Mischgenerator zum Empfangen einer Eingabe vom Kamerasystem und vom Empfänger, so daß die Kennungsdaten vom Empfänger zusammen mit dem vom Kamerasystem aufgenommenen Bild codiert werden, wobei der Mischgenerator Kombidaten erzeugt.

In der einfachsten Konfiguration der vorliegenden Erfindung werden die genannten Probleme der konventionellen Systeme und Verfahren dadurch gelöst, daß das erfindungsgemäße System ein oder mehrere Kennzeichen (z. B. ein Radiofrequenz-(RF-)Kennzeichen, ein magnetisches Kennzeichen, eine Smart Card, einen Strichcode, biometrische Identifikationsdaten usw.) zum Objekt enthält, die nicht entfernt werden können, ohne daß sie zerstört werden. Jedes Kennzeichen besitzt eine andere oder eindeutige Kennung.

In der exemplarischen Ausführungsform, in der es um Reparaturen an Kraftfahrzeugen geht, werden vorzugsweise mehrere Kennzeichen an verschiedenen Positionen des Fahrzeugs angebracht, so daß mindestens ein Kennzeichen einen typischen Verkehrsunfall übersteht.

Bei der Begutachtung des Schadens wird ein Foto aufgenommen, das aus einer Mischung aus optischen und Radiofrequenz-Identifikationsdaten (RFID) besteht. Um ein sol-

ches Bild zu erzeugen, ist die Kamera auf die beschädigten Teile des Fahrzeugs gerichtet, wobei vorzugsweise jedes beschädigte Teil ein Kennzeichen enthält, so daß die Kennung bei der Aufnahme des optischen Fotos gelesen und als "Wasserzeichen" für die Authentifizierung in das Bild eingefügt werden kann. Nach der Reparatur wird wieder mit der gleichen Kamera und dem gleichen RF-Lesegerät ein aus optischen und RFID-Daten zusammengesetztes Foto aufgenommen und dem Versicherungsunternehmen zusammen mit dem Originalfoto zum Vergleich der Fotos (und der optischen Signaturen der Kennzeichen) vorgelegt.

Außerdem sei erwähnt, daß auch eine Vorrichtung zur Einfügung eines Zeitstempels und/oder zur Entfernungsmessung vorhanden sein kann. So kann z. B. ein Lichtstrahl wie in einem Entfernungsmesser verwendet werden. Alternativ könnte auch ein akustischer Sensor verwendet werden, um den Abstand der Kamera vom Objekt zu messen. Eine solche Entfernungsmessvorrichtung bietet eine höhere Zuverlässigkeit und dient dazu, die Verwendung von Relaisstationen und ähnlichem zur Aufnahme der betrügerischen Bilder zu verhindern, die typischerweise fern vom wirklichen Objekt positioniert sind.

Außerdem bietet die vorliegende Erfindung ein System und ein Verfahren zur Authentifizierung von Informationen über ein Objekt, indem gleichzeitig mindestens zwei Eigenschaften eines Objekts und möglicherweise seiner Umgebung extrahiert werden, z. B. das Foto und die Temperatur, und diese Informationen zusammen mit Hilfe eines geheimen Schlüssels in einer Kombidatei chiffriert werden. Die chiffrierte Information kann einem fernen Benutzer dieser Information durch Dechiffrierung entweder mit einem veröffentlichten oder mit einem geheimen Schlüssel zur Verfügung gestellt werden.

So liefert z. B. wie erwähnt ein Foto eines Objektes einer dritten Partei Informationen über das Objekt; diese Informationen sind aber unter Umständen nicht authentisch, trotz Authentifizierung des Fotos beispielsweise durch ein Wasserzeichen, da das Foto von einem betrügerischen Modell des Objekts oder von einem Computerbildschirm, und nicht vom Objekt selber aufgenommen worden sein kann. Durch Kombination der fotografischen Abbildung mit anderen Arten der Erfassung ist eine wesentlich bessere Authentifizierung möglich. Dies gilt auch für Bilder, die von einer Videokamera aufgenommen werden. Außerdem muß die primäre Informationsquelle nicht visueller Natur sein, und die Erfindung erhöht so die Glaubwürdigkeit einer Aufzeichnung.

Eine der Eigenschaften des Objekts kann seine durch ein Kennzeichen bestätigte Identität sein. Durch gleichzeitige Erfassung (und Chiffrierung) der RF-Identifikationsdaten von einem identifizierenden Kennzeichen, das in das Objekt eingebettet oder an das Objekt angehängt sein kann, und anderen erfaßten Informationen läßt sich ein größeres Vertrauen in die Beziehung zwischen den gemessenen Daten und dem speziell identifizierten Objekt erreichen.

Außerdem kann die vorliegende Erfindung zerbrechliche Wasserzeichen zur Authentifizierung der Beziehung zwischen den angeblich aus einem physischen Objekt extrahierten Daten und dem Objekt selber verwenden. Diese Erfindung gibt den Benutzern von Informationen über physische Objekte mehr Vertrauen in die Authentizität dieser Information. Die Erfindung verwendet vorzugsweise zerbrechliche Wasserzeichen mehrerer gleichzeitig erstellter Dateien. Der Verifikationsprozeß kann entweder mit veröffentlichten Schlüsseln oder mit geheimen Schlüsseln oder mit einer Kombination beider Schlüsselarten durchgeführt werden.

KURZBESCHREIBUNG DER ZEICHNUNGEN

Die genannten und andere Aufgaben, Aspekte und Vorteile der Erfindung werden am besten aus der nachstehenden, ausführlichen Beschreibung einer bevorzugten Ausführungsform in Verbindung mit den Zeichnungen ersichtlich. Die Zeichnungen haben folgenden Inhalt:

Fig. 1 ist ein schematisches Diagramm eines Systems gemäß einer ersten bevorzugten Ausführungsform der vorliegenden Erfindung.

Fig. 2 zeigt ein erfindungsgemäßes System.

Fig. 3 ist ein Diagramm der Chiffrierung von zwei Datentypen von einem Objekt, um ein authentifiziertes Bild zu erzeugen.

Fig. 4 zeigt ein Kamerasystem mit Mitteln zur Entfernungsmessung und/oder zur Messung physikalischer Eigenschaften eines Objekts.

Fig. 5 zeigt ein Kennzeichen 501 mit mehreren Dipolen zur Verwendung mit der vorliegenden Erfindung.

AUSFÜHRLICHE BESCHREIBUNG BEVORZUGTER AUSFÜHRUNGSFORMEN DER ERFINDUNG

In den Zeichnungen, und speziell in Fig. 1, ist ein System 100 gemäß einer ersten bevorzugten Ausführungsform der vorliegenden Erfindung dargestellt.

Wie hier zu sehen ist, enthält das System 100 mindestens ein Kennzeichen 101, das einem Objekt 102 zugeordnet (z. B. angehängt, enthalten, befestigt usw.) ist. Vorzugsweise sind dem Objekt 102 mehrere Kennzeichen 101 zugeordnet, um eine höhere Zuverlässigkeit zu gewährleisten. Vorzugsweise handelt es sich bei den Kennzeichen um Radiofrequenzidentifikations-Kennzeichen (RFID-Kennzeichen), die der Umgebung ausgesetzt und für das Abbildungssystem sichtbar sind, so daß ein Bild vom Kennzeichen aufgenommen werden kann. Die Kennzeichen sind mit Informationen codiert, die zur Identifikation speziell des Fahrzeugs, an dem sie befestigt sind, dienen. Wie bereits erwähnt bewirkt jeder Versuch, die Kennzeichen zu ändern, zu entfernen und/oder an einem anderen Fahrzeug zu befestigen, daß die Kennzeichen zerstört oder unbrauchbar werden (z. B. durch Nullsetzung).

Die Kennzeichen können somit mit dem Objekt verknüpft, an das Objekt angehängt, in dem Objekt enthalten oder in das Objekt eingebettet sein. Die verwendeten Kennzeichen können entweder Eigenentwicklungen sein oder die gleichen oder ähnliche Kennzeichen wie die in einer Vielzahl von Entgegenhaltungen, z. B. in der US-Patentschrift Nr. 5,682,143 von Brady et al., der US-Patentschrift Nr. 4,063,229 von Welsh et al., der US-Patentschrift Nr. 4,242,663 von Slobodin und der US-Patentschrift Nr. 4,646,090 von Mawhinney, beschrieben; die genannten Patentschriften sind alle durch Bezugnahme Teil des vorliegenden Dokuments. Außerdem sind Kennzeichen von verschiedenen Quellen kommerziell zu beziehen, z. B. von Motorola, Texas Instruments, usw. Darüber hinaus können zusätzlich oder alternativ zu den oben beschriebenen noch andere Arten von Kennzeichen verwendet werden, z. B. magnetische Kennzeichen, RF-Kennzeichen gemäß US-Patentschrift Nr. 5,581,257 mit dem Titel "Radio Frequency Automatic Identification System" von Greene et al., die durch Bezugnahme Teil des vorliegenden Dokuments ist, usw. In anderen Anwendungen kann es sich bei den Kennzeichen auch um eine Smart Card, einen Strichcode, eine biometrische Identifikation usw. handeln. Für die exemplarische Ausführungsform, die im folgenden erläutert wird, wird der Bequemlichkeit halber angenommen, daß das Kennzeichen ein RFID-Kennzeichen ist.

Ein Empfänger/Kennzeichenlesegerät **103** (z. B. ein Radiofrequenz-Empfänger/Kennzeichenlesegerät) mit einer Antenne **103a** steht für die Abfrage bzw. das Lesen der RFID-Kennzeichen **101** zur Verfügung.

Ein Kamerasystem **104** (z. B. eine digitale Kamera wie eine CCD-Kamera o. ä.) hat die Aufgabe, Bilder vom Objekt **102** einschließlich der Kennzeichen **101** aufzunehmen. Die Kamera **104** ist operativ mit dem RF-Empfänger **103** gekoppelt, so daß wenn die Kamera ein Bild von dem gewünschten Objekt einschließlich der Kennzeichen aufnimmt, die Kennzeichen simultan vom RF-Empfänger **103** abgefragt und gelesen werden.

Ein Mischgenerator **105** empfängt Eingangssignale von der Kamera **104** und dem Kennzeichenlesegerät **103**.

Speziell wird die Tag-Identitätsinformation vom RF-Lesegerät **103** zusammen mit einem Zeitstempel (z. B. der Zeit der Ausgabe des Abfrageimpulses und der Zeit des Empfangs der Abfrageinformation des/der Tags) und anderen gewünschten Informationen codiert, z. B. mit der Brennweite der Kamera **104** oder mit einer Prüfsumme (z. B. möglicherweise verschlüsselt oder unverschlüsselt) des von der digitalen Kamera aufgenommenen Bildes.

Als Ergebnis generiert der Mischgenerator **105** die Kombidaten. Die codierten Daten können als angehängte Signatur hinzugefügt werden wie z. B. in der US-Patentschrift 5,499,294, die in ihrer Gesamtheit durch Bezugnahme Teil des vorliegenden Dokuments ist, oder als "zerbrechliches Wasserzeichen".

Ein unsichtbares Wasserzeichen ist eine Veränderung der Datei, die für einen Menschen kaum oder gar nicht erkennbar ist, aber von einer Maschine wie z. B. einem Computer festgestellt werden kann. Das Wasserzeichen sollte im wesentlichen nur für den Computer sichtbar sein. Das allgemeine Prinzip einer solchen Markierung durch Wasserzeichen ist z. B. in "Digital Watermarking for Highquality Imaging", von M. M. Yeung et al., Proceedings of the IEEE Signal Processing Society Multimedia Workshop, Princeton, New Jersey, 1997, beschrieben worden. Es können zerbrechliche Wasserzeichen (z. B. Wasserzeichen, anhand derer ein Benutzer erkennen kann, daß ein Bild authentisch ist und nicht verändert wurde) benutzt werden. Anstelle von Wasserzeichen kann man einem Bild auch eine Authentifikationsnachricht anhängen wie in der US-Patentschrift Nr. 5,499,294 von Friedman, die durch Bezugnahme Teil des vorliegenden Dokuments ist und oben erwähnt wurde.

Um zu verhindern, daß das RF-Lesegerät Kennzeichen liest, die nicht an das Objekt **102** angehängt sind, ist die Antenne im RF-Lesegerät vorzugsweise eine Richtantenne, und die Bewegung von Antenne/RF-Empfänger ist mit der Bewegung der digitalen Kamera **104** gekoppelt. Auf diese Weise empfängt die Richtantenne vorzugsweise RF-Signale nur aus der Richtung, in die die optische Kamera zeigt, wodurch sichergestellt wird, daß die optischen Bilddaten und die RF-Daten vom gleichen Ort stammen.

Abwandlungen der ersten bevorzugten Ausführungsform

Neben der obigen bevorzugten Ausführungsform, die in Fig. 1 dargestellt ist, können im Sinne und Schutzzumfang der vorliegenden Erfindung folgende Abwandlungen vorgenommen werden. Der besseren Verständlichkeit wegen und wie in Fig. 2 zu sehen ist, ist ein Blockdiagramm eines Systems **200** mit den folgenden Abwandlungen gegenüber System **100** dargestellt. Da solche Abwandlungen optional zu der Basiskonfiguration in Fig. 1 hinzugefügt werden können, sind sie mit gestrichelten Linien gezeichnet. Außerdem sei darauf hingewiesen, daß die im folgenden beschriebenen Abwandlungen einzeln oder in Kombination vorkommen

können, um größere Vorteile zu erreichen.

Beispielsweise kann das System **200** neben den Kennzeichen **101**, dem RF-Empfänger **103**, der Kamera **104** und dem Mischgenerator **105** eine Vorrichtung **106** (z. B. einen Verzögerungssensor oder ein Verzögerungserkennungs-Subsystem **106**) enthalten, um die Verzögerungszeit zwischen der Initialisierung des RF-Leseimpulses und deren Empfang (z. B. durch das Kennzeichenlesegerät **104**) zu messen. Auf diese Weise kann festgestellt werden, ob RF-Relaisstationen verwendet wurden, um das System auszuwickeln und ein falsches Bild zu erzeugen.

Da die Geschwindigkeit elektromagnetischer Wellen 3×10^8 Meter pro Sekunde beträgt, sollte für ein Bild von dem reparierten Fahrzeug ein Abstand von ca. 3 bis 5 Metern zwischen der Kamera und dem Fahrzeug erforderlich sein. Dieser Abstand kann anhand der Brennweite der optischen Kamera **104** gemessen werden. So liegt die Verzögerung gegenüber einem Initialisierungssignal in der Größenordnung von ca. 20 bis 33 Nanosekunden. Wesentlich davon abweichende (z. B. längere) Zeiten würden darauf hinweisen, daß eine Relaisstation verwendet wurde, um die RF-Signale von einem anderen Ort herzuholen.

Die Verzögerungszeiten werden vorzugsweise ebenfalls aufgezeichnet und vom Mischgenerator **105** in die zusammengesetzten Daten codiert. Der Verzögerungssensor **106** könnte vorteilhafterweise in Verbindung mit dem oben erwähnten Zeitstempelsensor/-Chiffrierer **109** verwendet werden.

Eine andere Abwandlung der bevorzugten Ausführungsform aus Fig. 1 besteht darin, daß die Codierung der Daten vom RF-Kennzeichen und andere Informationen vom Mischgenerator **105** in eine Chiffriervorrichtung **107** eingegeben werden können, mit Hilfe einer Kryptographie mit veröffentlichtem oder geheimem Schlüssel, wie z. B. in der US-Patentschrift 5,499,294 von Friedman beschrieben, die durch Bezugnahme Teil des vorliegenden Dokuments sind.

Auf diese Weise werden die codierten Daten entweder mit einem veröffentlichten oder mit einem geheimen Schlüssel weiter verschlüsselt, um eine weitere Stufe der Zuverlässigkeit und Sicherheit hinzuzufügen. In beiden Fällen werden bekanntlich die betreffenden Dechiffrierschlüssel benötigt, um die Codierungsdaten zu dechiffrieren. Ein exemplarisches Subsystem **300** zur Chiffrierung ist in Fig. 3 dargestellt. Darin werden ein Kamerabild **302** eines Objekts und vorgegebene Eigenschaften **304** des Objekts sowie Informationen des geheimen Schlüssels in eine Chiffriervorrichtung **308** eingegeben. Die Chiffriervorrichtung **308** erzeugt dann ein chiffriertes Bild **310** zur Authentifizierung. Eine Beschreibung der speziellen Kryptographieverfahren (z. B. SK/PK-Paare und Prüfsummenfunktionen) finden sich im "Handbook of Applied Cryptography", Alfred J. Menezes et al., CRC Press, 1997.

In Fig. 3 ist ein digitales Bild von einem Objekt die Reflexion von Photonen an einer Oberfläche dargestellt, die vom digitalen Kamerasystem **104** aus Fig. 1 oder von Standard-Fotografiermaterial aufgezeichnet wird. Das Bild stellt den momentanen Zustand des Objekts dar und wird oft zur Kontrolle verwendet. So kann beispielsweise wie oben erwähnt ein Foto des Unfallschadens an einem PKW zur Prüfung eines Versicherungsanspruchs verwendet werden. Das Bild kann manipuliert werden.

Deshalb wird in Fig. 3 ein dreidimensionales Objekt abgetastet, und mindestens zwei Dateien, die das Bild **302** und eine Eigenschaft des Objekts **304** enthalten, werden von der Chiffriervorrichtung **306** zusammen chiffriert wie in Fig. 3. Dabei kann es sich um das Kamerabild und eine interferometrische Messung (entweder mittels elektromagnetischer Wellen oder mittels Schallwellen) des Objekts handeln. Die

kombinierte Datei 310 gibt die Gewißheit, daß diese Datei das tatsächliche Objekt darstellt, und daß es sich nicht um eine Manipulation eines simulierten Objekts oder ein nachträglich von einem Bildschirm oder einem anderen zweidimensionalen Medium abfotografiertes Bild handelt.

In Fig. 4 ist ein Beispiel für die Bereitstellung solcher Informationen dargestellt. Das Objekt 406 ist eine Weinflasche, die mit der digitalen Kamera 400 fotografiert werden kann. Um zu kontrollieren, daß das Bild tatsächlich ein Bild von dem dreidimensionalen Objekt ist, um das es sich angeblich handelt, werden mit einer Entfernungs- und oder Längenmeßvorrichtung 400 der Abstand vom Objekt und/oder die Abmessungen des Objekts gemessen. Eine solche Vorrichtung kann elektromagnetische Wellen und/oder Schallwellen verwenden, die von der Kamera ausgesandt werden und deren Echo von der Kamera im wesentlichen zum Zeitpunkt der Bildaufnahme empfangen werden. Außerdem enthält die Weinflasche ein elektronisches Kennzeichen 408, und diese Information wird ebenfalls an ein RFID-Kennzeichenlesegerät 410 gesendet und von der Kamera 400 aufgezeichnet. Alle Informationen werden wie in Fig. 3 kombiniert und chiffriert, um das Objekt darzustellen.

In dem Beispiel aus Fig. 4 wird nur die Entfernung herangezogen; es können jedoch viele Aspekte und Eigenschaften des Objekts aufgezeichnet werden, einschließlich, aber nicht beschränkt auf: Gewicht, Dichte mit Darstellung dreidimensionaler Hohlräume im Objekt, topografische Oberflächenmessungen, Vibrationsniveau, Schallemissionen, Radioaktivität, Kernspinresonanz (NMR), Infrarotspektrum, elektromagnetische Strahlung usw.

Wieder in Fig. 2 ist eine weitere Abwandlung des Basissystems aus Fig. 1 zu sehen, bei der die Kamera 104 mit einer Zoom-Linse 108 ausgestattet ist und automatisch mehrere Bilder mit verschiedenen (vorzugsweise zufällig gewählten) Zoom-Einstellungen aufgenommen werden. Die Zoom-Einstellungen werden in eines der Bilder oder in beide Bilder codiert.

Eine andere Abwandlung beinhaltet ein System wie das obige, in dem das Lesegerät ebenfalls ein RF-Kennzeichen 101 enthält, so daß sowohl das RF-Kennzeichen des Lesegeräts als auch das des Objekts 102 bei der Aufnahme des Bildes aufgezeichnet werden. Diese Kombination macht es schwieriger, das Lesegerät 103 und die Kamera 104 in betrügerischer Absicht nachzuahmen. Außerdem könnte die digitale Kamera mit dem Kennzeichen für eine bestimmte Werkstatt/Stelle, die das Foto aufnimmt, registriert werden, um eine noch höhere Zuverlässigkeit und Sicherheit zu erreichen.

In einer zusätzlichen Abwandlung des obigen Systems gibt es mindestens ein Kennzeichen 501 (und vorzugsweise mehrere Kennzeichen 510), das anstelle der Siliziumtechnologie eine Reihe von Dipolen enthält, und das auf analoge Weise gelesen wird. Eine solche Implementierung von Kennzeichen wird in der US-Patentschrift 5.581.257, "Radio Frequency Automatic Identification System" von Greene et al. beschrieben, die durch Bezugnahme Teil des vorliegenden Dokuments ist. In solchen Kennzeichen 501 sind Drähte 502 z. B. in einer Papierverpackung oder einem Gehäuse 503 (z. B. aus Pappmaché) zufällig verteilt. Solche Kennzeichen können nicht einfach durch Lesen dupliziert werden. Die Signatur für diese Kennzeichen wird vorher aufgezeichnet und in einer Datenbank gespeichert (z. B. bei dem Versicherungsunternehmen, usw.) Die Signatur des Kennzeichens wird mit Hilfe von Radiowellen aufgezeichnet, aber auf eine andere Weise als bei einem typischen RFID-Kennzeichen auf Siliziumbasis gelesen. Wegen der zufälligen Anordnung kann das vorher aufgezeichnete Signal nicht nachgemacht werden, wenn die Konfiguration der

Drähte verteilt wird geändert wird.

Eine weitere Abwandlung besteht darin, eine Zeitstempelabtastr- und Chiffriervorrichtung 109 zu integrieren, um ein Zeitstempel abzutasten und in das vom Kamerasystem aufgenommene Bild zu chiffrieren. Der Zeitstempel bezeichnet einen Zeitpunkt, an dem das Bild vom Kamerasystem aufgenommen worden ist, und bietet eine weitere Stufe der Authentizität für das Bild.

Auf diese Weise hält die vorliegende Erfindung potentielle Betrüger davon ab, ein Bild von einem Objekt aufzunehmen, das nicht das angeblich dargestellte Objekt ist, z. B. für Versicherungszwecke. Die Abschreckungswirkung wird erreicht, weil solche betrügerische Aktivitäten sehr zuverlässig entdeckt werden. Die sehr zuverlässige Erkennung, die durch die vorliegende Erfindung möglich wird, wirkt abschreckend gegen betrügerische Aktivitäten wie die Aufnahme des Bildes von einem unbeschädigten Fahrzeug, das ähnlich aussieht wie das Unfallfahrzeug, und die Vorlage eines solchen Bildes bei einem Versicherungsunternehmen, um Geld für eine in Wirklichkeit gar nicht ausgeführte (oder in manchen Fällen nicht einmal notwendige) Reparatur zu kassieren.

Außerdem verhindert die vorliegende Erfindung den Aufbau von Relaisstationen, die ein falsches oder gefälschtes fernes Bild übertragen können, oder bietet zumindest eine Abschreckung dagegen.

Auch wenn die Erfindung anhand bevorzugter Ausführungsformen beschrieben worden ist, ist dem Fachmann klar, daß die Erfindung mit Abwandlungen im Sinne und innerhalb des Geltungsumfangs der angefügten Ansprüche realisiert werden kann.

Zum Beispiel könnten andere Parameter wie Geruch oder Geräusch gemessen werden, sofern das Meßinstrument (z. B. ein "Schnüffler" oder ein Hörinstrument oder ähnliches) ein entsprechendes Kennzeichen enthält. Für die Zuverlässigkeit und Authentizität könnte eine Darstellung des Parameters auf dem Foto plziert werden.

Außerdem sei angemerkt, daß der oben beschriebene Zeitstempel mit einem ausgestrahlten nationalen Rundfunksignal, z. B. vom National Institute of Standards and Technology (z. B. über dessen Rundfunk-Rufbuchstaben "WWV") oder über ein Netzwerk wie das Internet indexiert sein kann. Eine solche Zeit würde in das Foto oder Bild von dem betreffenden Objekt chiffriert, um eine hohe Zuverlässigkeit der Authentifizierung zu erreichen.

Außerdem wurden die Kennzeichen als durch ein externes Feld abgefragte Kennzeichen beschrieben. Zusätzlich oder alternativ zu den passiven Kennzeichen könnten "aktive" elektronische Kennzeichen benutzt werden, um Identifikationsdaten auszusenden.

Außerdem wurde in der Beschreibung der exemplarischen, nicht einschränkend zu verstehenden Ausführungsform und ihren Abwandlungen ein Auto angesprochen; die vorliegende Erfindung kann aber genauso gut auch auf andere Objekte angewandt werden, z. B. auf Unterhaltungselektronik aus der Massenproduktion wie Fernsehgeräte, Videorecorder und ähnliches, andere Kraftfahrzeuge wie LKWs, Motorräder, und Boote, Flugzeuge, Kunstwerke, teure Kleidung usw. Viele unbelebte Objekte würden von der Erfindung erheblich profitieren.

Außerdem könnte das erfindungsgemäße System auch leicht zur Identifikation belebter Objekte (z. B. Menschen, Tiere usw.) verwendet werden. In einem solchen Fall kann das belebte Objekt identifiziert werden, indem ein Bild von dem belebten Objekt aufgenommen wird, während gleichzeitig andere Daten (z. B. die Bestätigung biometrischer Informationen wie Iris/Netzhautmuster, Zahnschema usw.) erfaßt werden. Außerdem können die belebten Objekte ein

Kennzeichen tragen (z. B. ein RF-Kennzeichen, ein Magnet-Kennzeichen, eine Smart Card, einen Strichcode, eine biometrische Kennung, usw.). Auf diese Weise können mit der vorliegenden Erfindung belebte und unbelebte Objekte leicht authentifiziert werden.

Patentansprüche

1. Ein System zur Authentifizierung eines Bildes von einem Objekt, enthaltend:
mindestens eine Kennung, die dem Objekt zugeordnet ist;
einen Empfänger zur Abfrage der mindestens einen Kennung, um Identifikationsdaten zu erzeugen;
ein Kamerasystem zum Aufzeichnen eines Bildes von dem Objekt einschließlich der mindestens einen Kennung; und
einen Mischgenerator zum Codieren der Identifikationsdaten aus dem Empfänger in Form codierter Daten, zusammen mit dem vom Kamerasystem aufgenommenen Bild, und zum Generieren von zusammengesetzten Daten.
2. Das System nach Anspruch 1, wobei die mindestens eine Kennung eine Radiofrequenzkennung (RF-Kennung) umfaßt; und/oder wobei die mindestens eine Kennung eine biometrische Kennung umfaßt; und/oder wobei die mindestens eine Kennung mindestens einen Strichcode und eine Smart Card umfaßt.
3. Das System nach Anspruch 1, wobei der Empfänger mindestens einen Radiofrequenzempfänger (RF-Empfänger) umfaßt.
4. Das System nach Anspruch 1, wobei die mindestens eine Kennung mindestens für das Objekt oder ein Merkmal des Objekts eindeutig ist; und/oder wobei mehrere Kennungen an das Objekt angebracht sind; und/oder wobei das Kamerasystem eine digitale Kamera umfaßt; und/oder wobei die codierten Daten dem Bild als Signatur oder als Wasserzeichen hinzugefügt werden.
5. Das System nach Anspruch 1, wobei der Empfänger eine Richtantenne umfaßt, um zu verhindern, daß der Empfänger eine andere als die mindestens eine Kennung liest, so daß die Richtantenne Radiofrequenzsignale (RF-Signale) von Kennungen nur in einer Richtung, in die das Kamerasystem zeigt, empfängt.
6. Das System nach Anspruch 1, wobei die Identifikationsdaten mindestens eine Entfernung zwischen dem Kamerasystem und dem Objekt oder eine Brennweite des Kamerasystems enthält.
7. Das System nach Anspruch 1 oder 6, außerdem umfassend:
ein an den Empfänger angeschlossenes Verzögerungsmessungs-Subsystem zum Messen einer Verzögerungszeit zwischen der Initialisierung eines auf das Objekt gerichteten Impulses des Empfängers und dessen Empfang durch den Empfänger.
8. Das System nach Anspruch 7, wobei die Verzögerungszeit aufgezeichnet und vom Mischgenerator in die zusammengesetzten Daten codiert werden.
9. Das System nach Anspruch 1, außerdem umfassend:
eine an den Mischgenerator angeschlossene Chiffriervorrichtung, wobei die Codierung der Identifikationsdaten aus der mindestens einen Kennung und vorgegebenen Informationen aus dem Mischgenerator in die

Chiffriervorrichtung eingegeben wird, unter Verwendung eines veröffentlichten Schlüssels und eines privaten Schlüssels.

10. Das System nach Anspruch 1, wobei das Kamerasystem ein Zoom-Linsensystem enthält und automatisch mehrere Bilder mit verschiedenen Zoom-Einstellungen des Zoom-Linsensystems erzeugt.

11. Das System nach Anspruch 10, wobei die Zoom-Einstellungen zufällige Zoom-Einstellungen umfassen; und/oder wobei die Zoom-Einstellungen in mindestens eines der mehreren Bilder codiert werden.

12. Das System nach Anspruch 1, wobei der Empfänger eine hinzugefügte Kennung enthält, so daß sowohl die Kennung des Empfängers als auch die mindestens eine Kennung des Objekts aufgezeichnet werden, wenn das Kamerasystem ein Bild von dem Objekt aufnimmt; und/oder

wobei die mindestens eine Kennung mehrere Dipole enthält; und/oder

wobei die mindestens eine Kennung Silizium umfaßt; und/oder

wobei die mindestens eine Kennung ein Radiofrequenzidentifikations-Kennzeichen umfaßt; und/oder

wobei das Bild mit einem Zeitstempel codiert wird; und/oder

wobei das Objekt ein unbelebtes Objekt umfaßt; und/oder

wobei das Objekt ein Kraftfahrzeug oder ein Kunstwerk umfaßt; und/oder

wobei das Objekt ein belebtes Objekt umfaßt; und/oder wobei die mindestens eine Kennung eine fälschungssichere Kennung umfaßt, so daß eine Änderung oder Entfernung der mindestens einen Kennung diese ungültig macht.

13. Das System nach Anspruch 1, wobei eine Signatur, die der mindestens einen Kennung entspricht, vorher aufgezeichnet wird.

14. Das System nach Anspruch 13, wobei die Signatur der mindestens einen Kennung mit Hilfe von Radiofrequenzen vorher aufgezeichnet wird.

15. Das System nach Anspruch 1, außerdem mit Mitteln zum Chiffrieren eines Zeitstempels in dem Bild, wobei der Zeitstempel eine Zeit angibt, zu der das Bild vom Kamerasystem aufgenommen wurde; und/oder außerdem mit Mitteln zum Abtasten einer Zeit, zu der das Bild vom Kamerasystem aufgenommen wird, zum Einbetten eines Zeitstempels in das Bild und zum Chiffrieren des Bildes einschließlich des Zeitstempels.

16. Ein Verfahren zur Authentifizierung eines Objekts, umfassend:

einem Zuordnen mindestens einer Kennung zu dem Objekt;

einem Abfragen der mindestens einen Kennung, um Identifikationsdaten zu erzeugen;

einem Aufzeichnen eines Bildes von dem Objekt einschließlich der mindestens einen Kennung; und
einem Codieren der Identifikationsdaten, die auf der Abfrage der mindestens einen Kennung basieren, zusammen mit dem aufgezeichneten Bild, um Kombidaten zu erzeugen.

17. Das Verfahren nach Anspruch 16, wobei das Objekt ein unbelebtes Objekt umfaßt.

18. Das Verfahren nach Anspruch 17, wobei das Objekt ein Kraftfahrzeug oder ein Kunstwerk umfaßt.

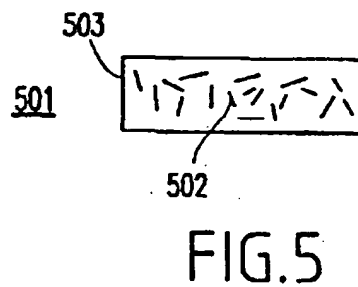
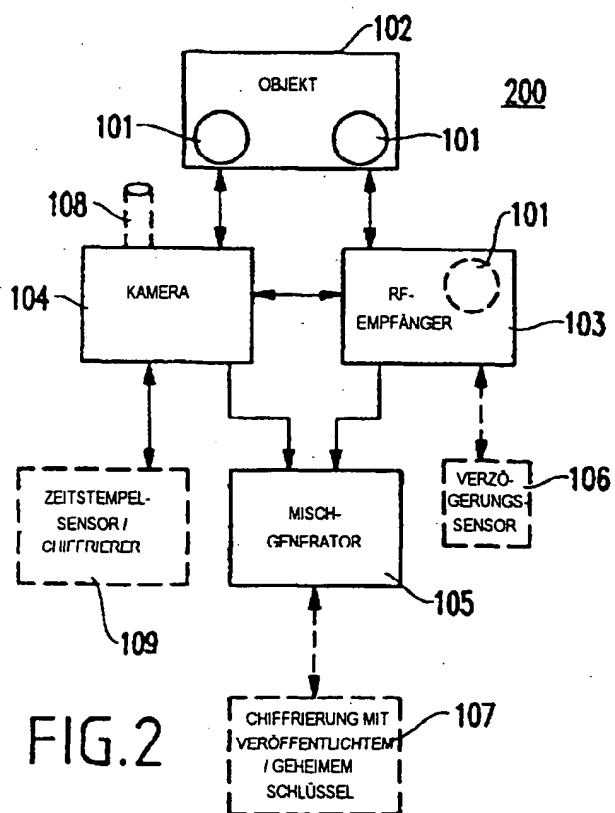
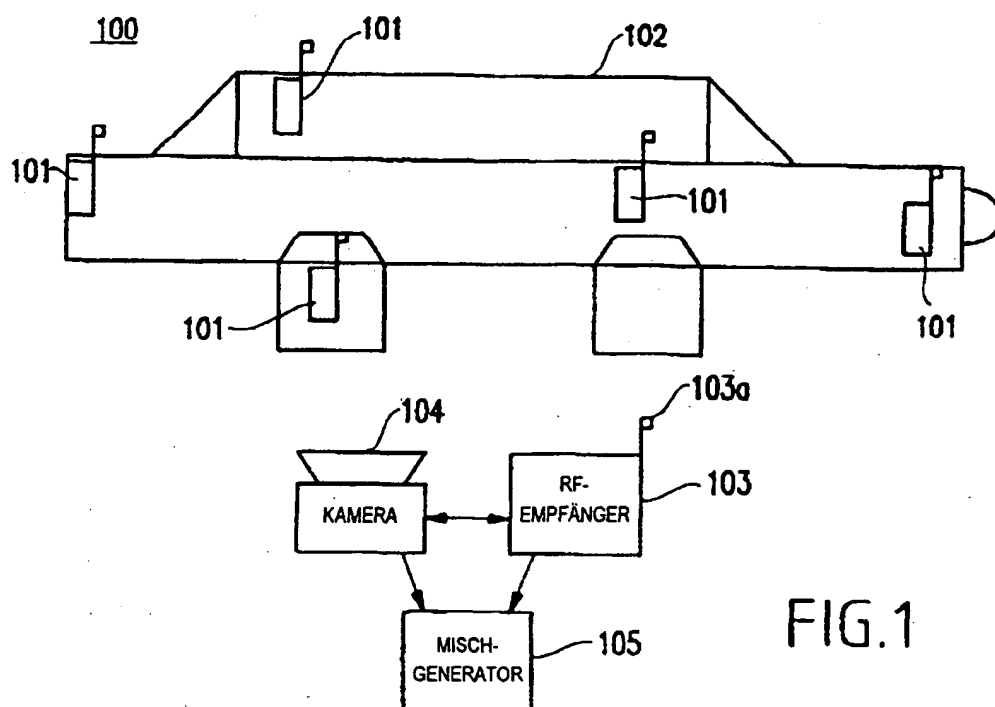
19. Das Verfahren nach Anspruch 16, wobei das Objekt ein belebtes Objekt umfaßt; und/oder wobei die mindestens eine Kennung eine Radiofre-

quenzkennung umfaßt; und/oder
wobei die mindestens eine Kennung eine biometrische Kennung umfaßt; und/oder
wobei die mindestens eine Kennung einen Strichcode und/oder eine Smart Card umfaßt; und/oder
wobei die mindestens eine Kennung mindestens für das Objekt oder ein Merkmal des Objekts eindeutig ist; und/oder
wobei die mindestens eine Kennung eine fälschungssichere Kennung umfaßt und wobei das Verfahren außerdem die fälschungssichere Kennung als Reaktion auf eine Änderung und Entfernung der mindestens einen Kennung ungültig macht.
20. Ein Verfahren zur Authentifizierung eines Objekts, umfassend:
gleichzeitiges Extrahieren von mindestens zwei Arten von Informationen, die dem Objekt zugeordnet sind; gleichzeitig mit dem Extrahieren ein gemeinsames Chiffrieren der mindestens zwei Arten von Informationen; und
ein Dechiffrieren von mindestens zwei Arten von Informationen, um die Authentizität des Objekts zu verifizieren.
21. Das Verfahren nach Anspruch 20, wobei die Extrahierung die Aufzeichnung eines Bildes von dem Objekt und die Ermittlung einer intrinsischen physikalischen Eigenschaft des Objekts umfaßt.
22. Das Verfahren nach Anspruch 21, wobei das Bild eine Fotografie umfaßt und wobei die intrinsische Eigenschaft des Objekts eine topografische Messung der Oberfläche des Objekts beinhaltet; und/oder
wobei das Bild eine Fotografie umfaßt und wobei die mindestens eine intrinsische Eigenschaft eine magnetische Eigenschaft des Objekts beinhaltet.
23. Das Verfahren nach Anspruch 21, wobei das Bild eine Fotografie umfaßt und wobei die intrinsische Eigenschaft des Objekts die Dichte oder das Gewicht des Objekts beinhaltet.
24. Das Verfahren nach Anspruch 23, wobei die Dichte dreidimensionale Hohlräume in dem Objekt aufzeigt.
25. Ein Verfahren nach Anspruch 20, wobei eine der zwei Arten von Information eine elektromagnetische Strahlung des Objekts umfaßt; und/oder
wobei eine der beiden Arten von Information aus einem elektronischen Kennzeichen, das Identifikationsdaten aussendet, und aus einem passiven Kennzeichen, das bei Abfrage durch ein äußeres Feld eine der zwei Arten von Informationen enthüllt, stammt; und/oder
wobei mindestens eine der zwei Arten von Information in einer zeitlichen Reihenfolge angewendet wird; und/oder
wobei eine der mindestens zwei Arten von Information ein digitales Bild des Objekts umfaßt und das Objekt ein dreidimensionales Objekt umfaßt; und/oder
wobei das Objekt ein unbelebtes Objekt umfaßt; und/oder
wobei das Objekt ein Kraftfahrzeug oder ein Kunstwerk umfaßt; und/oder
wobei das Objekt ein belebtes Objekt umfaßt; und/oder
wobei die zwei Arten von Information eine Bildinformation des Objekts und biometrische Information, die dem Objekt eindeutig zugeordnet ist, enthalten; und/oder
wobei eine der zwei Arten von Information aus einer dem Objekt zugeordneten Radiofrequenzkennung

stammt; und/oder
wobei eine der zwei Arten von Information aus einer dem Objekt zugeordneten biometrischen Kennung stammt; und/oder
wobei eine der zwei Arten von Information von einem dem Objekt zugeordneten Strichcode und/oder einer dem Objekt zugeordneten Smart Card stammt; und/oder
wobei eine der zwei Arten von Information von mindestens einer dem Objekt zugeordneten Kennung stammt, die eine fälschungssichere Kennung umfaßt, und wobei das Verfahren außerdem die fälschungssichere Kennung als Reaktion auf eine Änderung und Entfernung der mindestens einen Kennung ungültig macht.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -



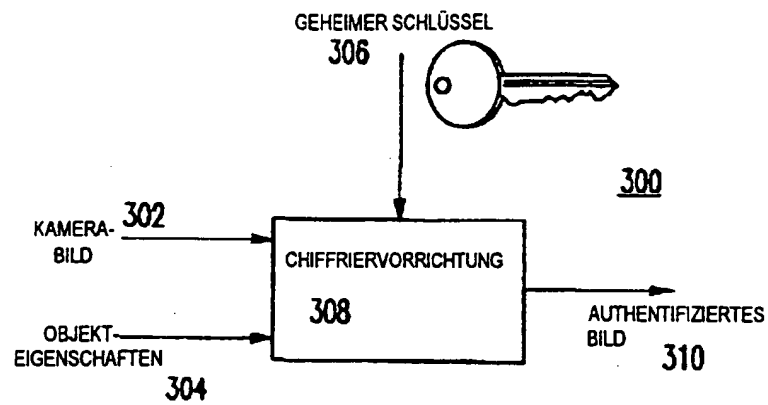


FIG.3

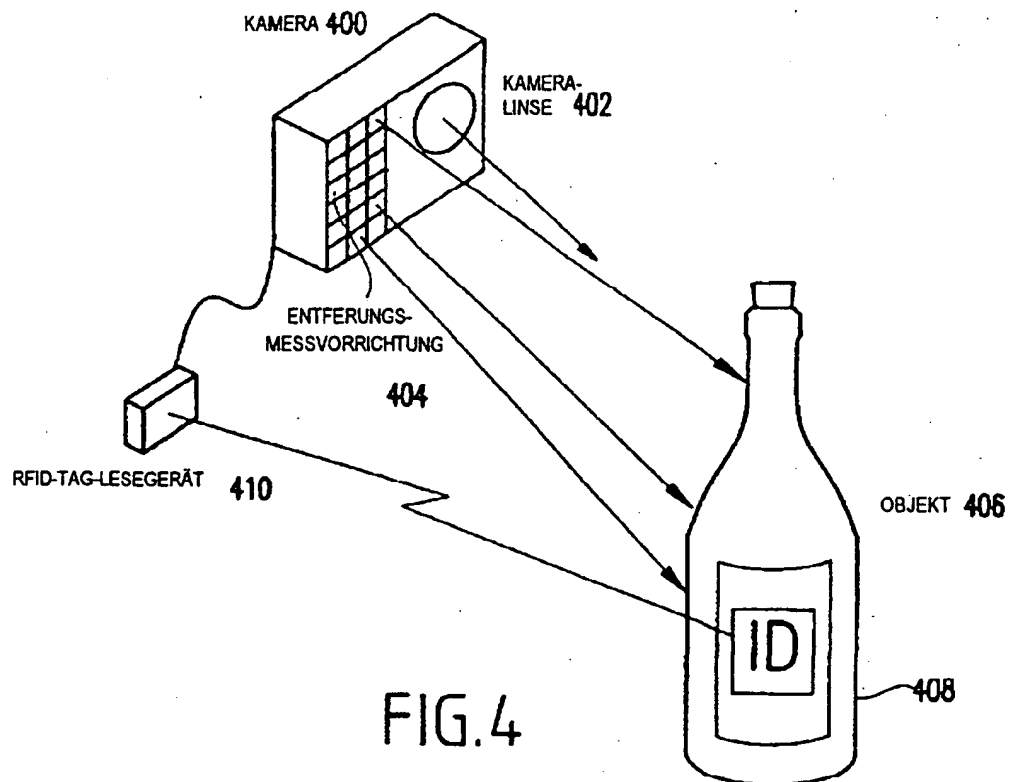


FIG.4